Capsule networks for low-data transfer learning

Andrew Gritsevskiy
agritsevskiy@gmail.com

Abstract

We propose a capsule network-based architecture for generalizing learning to new data with few examples. Using both generative and non-generative capsule networks with intermediate routing, we are able to generalize to new information over 25 times faster than a similar convolutional neural network. We train the networks on the multiMNIST dataset lacking one digit. After the networks reach their maximum accuracy, we inject 1-100 examples of the missing digit into the training set, and measure the number of batches needed to return to a comparable level of accuracy. We then discuss the improvement in low-data transfer learning that capsule networks bring, and propose future directions for capsule research.

1 Introduction

Unlike the human brain, which can learn from relatively few examples, neural networks have long required tens of thousands of examples to generalize to a new concept. A newborn, having seen a giraffe one or two times in its life, can immediately recognize the animal in any other place. A neural network, however, still requires thousands of giraffe images to have even a comparable level of accuracy. The field of transfer learning focuses on solving this problem, in which we propose a solution using a capsule network.

Capsule networks, first proposed by Sabour et al. [SFH17], are a recently developed type of neural network, in which groups of neurons, called capsules, learn certain properties about an object. Each capsule in a layer tries to predict how to maximize the activations of the higher-level capsules by choosing the amount of information to send to each capsule in the next layer. Deciding where the information is actually sent is determined by the agreement of the capsules’ predictions. Capsules, rather than simply passing along a scalar, maintain a vector of information about the object—where the length of the vector represents the probability that a certain object exists, while the values of the vector represent its instantiation parameters—anything from its orientation to stroke width to color. Each capsule uses a squash nonlinearity, which makes short vectors have a length close to 0 and long vectors have a length close to 1. However, where the capsules send their information is not decided purely by backpropagation. Instead, each layer undergoes several iterations of dynamic routing—the capsules try to predict the output of those in the next layer, and send information based on agreement. It is this procedure that allows capsule-based architectures to so effectively segment a scene into its underlying objects without considering parts of different objects to be spatially related. However, despite the potential present in capsule-based architectures, their accuracy on image segmentation tasks has not been considerably higher than that of their convolutional counterparts. In this paper, we demonstrate that capsule networks—in particular, generative capsule networks—provide a tremendous advantage over convolutional neural networks in the area of transfer learning, where they can learn segment a scene with unknown objects over 100 times faster than before, as well as achieve a significantly higher overall accuracy on an expanded dataset.
2 Architectures

We focus on three architectures in our paper—a regular convolutional neural network, a regular capsule network (as described in Sabour et al.), and a generative capsule network. The convolutional neural network consists of three convolutional layers and two fully-connected layers with softmax cross-entropy loss. The regular capsule network contains routing between the Primary Capsule layer and the Digit Capsule layer, as in the original paper. The generative capsule network uses what we call a memo architecture, which consists of convolving the images into the Digit Capsules, applying convolutional reconstruction, and classifying images based on the reconstruction (a detailed description of the setup and implementation can be found in Appendix I).

3 Methods

Our experiments were conducted on variations of the multiMNIST dataset, first described in Sabour et al [SFH17]. The task is to cleave overlapping MNIST images, such as those in Figure 1, into the two constituent digits. The three datasets we used, summarized in Table I, were as follows: first, we had a normal multiMNIST dataset with 200000 training examples of randomly overlapping MNIST images, with each image shifted uniformly randomly between 0 to 8 pixels relative to the other image. This also contained 10000 test examples of overlapping digits shifted by each of 0, 2, 4, 6, and 8 pixels relative to each other. Next, we had the subMMNIST dataset, which is identical in principle to the multiMNIST dataset, except the training data did not contain any examples with a certain single digit. One test set similarly lacked this certain digit; the second test set consisted of examples comprised of all ten digits. Finally, we also had the ldMMNIST dataset, which, instead of completely lacking a digit, contained only a small number of examples of that digit. Specifically, we had eight such ldMMNIST datasets, containing 1, 5, 10, 50, 100, 500, 1000, and 5000 examples, respectively. The test sets were identical to those of the subMMNIST dataset.

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Training set</th>
<th>Testing sets</th>
<th>Train/test examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>multiMNIST</td>
<td>Ten digits</td>
<td>Ten digits shifted from 0 to 8px</td>
<td>200000 total/10000 per test set</td>
</tr>
<tr>
<td>subMMNIST</td>
<td>Nine digits</td>
<td>Ten digits shifted from 0 to 8px</td>
<td>200000 total/10000 per test set</td>
</tr>
<tr>
<td>ldMMNIST</td>
<td>Ten digits, but one digit is only sampled from (1/10/50/100/...) examples</td>
<td>Ten digits shifted from 0 to 8px</td>
<td>200000 total/10000 per test set</td>
</tr>
</tbody>
</table>

Table 1: A summary of the three datasets used.

Figure 1: Three training images from the multiMNIST dataset. The first image contains a 0 overlapping with a 9, the second contains a 2 overlapping with a 5, and the third contains a 4 overlapping with a 0.

The experimental setup was essentially training the three different architectures on the subMMNIST dataset, and proceeding to inject the missing digit into the training data by switching to either the multiMNIST or the ldMMNIST datasets. Then, we would see how quickly each network could adjust to new data by reaching its pre-injection accuracy. We also analyzed the final accuracy it attained.
4 Experimental results

4.1 Generative capsule network and convolutional network

For our first comparison, we trained the convolutional network and the generative capsule network for 125,000 batches each on the subMMNIST dataset. Both networks achieved an accuracy of roughly 81%, with the capsGAN scoring slightly higher on the test set. After the 125,000 iterations, we injected the multiMNIST dataset, which contains all the digits, as well as the ldMMNIST-100 dataset, which contains all the digits but only 100 distinct examples of the tenth digit. It took the convolutional network 2700 iterations to reach its old accuracy, and it achieved less than an 82% final accuracy with the full injection, and an 88.4% final accuracy with the ld-100 injection. The generative capsule network adapted to the new data instantaneously (within 100 iterations), and achieved over a 96.3% peak accuracy with the full injection, and a 97.5% peak accuracy with the ld-100 injection, as shown in Table 3. A plot of the testing accuracy is shown in Figure 3, and the raw data is provided in Appendix II.

Table 2: The generative capsule architecture is achieves better accuracy at a faster rate when generalizing to new data, when compared to standard convolutional techniques.

<table>
<thead>
<tr>
<th>Architecture</th>
<th>Iterations to reach initial accuracy</th>
<th>Pre-injection accuracy</th>
<th>Peak accuracy on full test set with full injection</th>
<th>Peak accuracy on full test set with ld-100 injection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Convolutional</td>
<td>2700</td>
<td>80.7%</td>
<td>&lt;82%</td>
<td>88.4%</td>
</tr>
<tr>
<td>Generative capsule</td>
<td>&lt;100</td>
<td>81.9%</td>
<td>96.3%</td>
<td>97.5%</td>
</tr>
</tbody>
</table>

Thus, in experiments comparing the speed and effectiveness of adaptation to new data, the generative capsule model significantly outperformed conventional convolutional architectures, improving upon data generalization speed by over a factor of 25, and final accuracy by over 9 percentage points, both on full- and low-data injections.

4.2 Capsule network and convolutional network

We also wish to show that generative learning is not a requirement for capsule networks to generalize well to new data. In our second experiment, we train a convolutional network and a capsule network for 50,000 iterations each before injecting the full datasets, as well as the ld-1, ld-10, ld-50, and ld-100 test sets. Unlike the generative capsule network, the regular capsule network immediately achieves a higher accuracy while training, reaching 84.5% before injection, compared to the convolutional network’s 81.4%. After injection, the capsule network also outperforms the convolutional network with a 91.1% peak accuracy compared to the latter’s 86.5%, as plotted in Figure 4. The most interesting results were perhaps on the low-data injections—shockingly, a capsule network presented with 50 or 100 examples of a missing digit greatly outperformed the same network on the full dataset, by over a percentage point in accuracy. A complete summary of low-data training is described in Table 3 and Figure 5.

1In reality, the capsule network was only trained for 33000 iterations, but this should not have a significant effect on the results. We have considered the idea that if a convolutional network trains longer than its capsule counterpart, the L2 regularization may make the weights smaller and therefore less adaptive to new data. However, a capsule injection at 7500 iterations achieved virtually identical results, from which we conclude that this is not a significant issue.
Figure 3: A plot of the training accuracies of the generative capsule network (capsGAN) and the convolutional network (convnet) from iteration 100,000 to 135,000, with the injections occurring on the 125,000th iteration.

![Plot of training accuracies](image)

Figure 4: Testing accuracy of a capsule network and a convolutional network, before and after a full-data injection.

![Testing accuracy plot](image)
Table 3: The capsule net improves upon the convolutional network in every test of data generalization.

## Discussion

There are several major results to note about capsule networks. First, capsule networks, both standard and generative, are a significant improvement upon existing convolutional neural networks in the realm of generalizing to new data, steadily reaching improvements of nine percentage points (for generative networks) and three percentage points (for standard networks) over their convolutional counterparts after data injection. One major reason for this may be intrinsic to the structure of the capsule network itself—namely, it consists of ten “pathways” through which information about digits can be routed. If only nine digits are presented, as is the case initially, only nine of the ten pathways may be activated. When a new digit is presented, it does not activate any of the capsules in the existing routing pathways, and is thus sent through the previously unused one. Thus, we predict that capsule networks will have trouble generalizing to more data than channels available in the network, but further testing is required to verify this hypothesis. Furthermore, this may help explain the baffling result of a higher accuracy on a low-data injection (50/100 examples) than on a full-data injection—if there are fewer examples, it may become clearer to the network that this is a separate class of digit. If more examples are presented, it may have trouble classifying it as a new digit, and instead try to group each example into an existing class. Once again, further research is required to find the optimal amount of new data for the best possible generalization. However, it is still acutely intriguing that, even with convolutional networks, and, to a greater extent, with capsule networks, less data in transfer learning may have an unprecedented positive impact.

Another interesting point is the difference between generative capsule networks and regular capsule networks. Although generative capsule networks are both slower and worse at training, achieving a pre-injection accuracy of several percentage points less and taking thousands of iterations longer to achieve it, they nevertheless perform much better after injection—achieving as high as a 97.5% accuracy on the multiMNIST test set, improving upon the 95.0% currently achieved by Sabour et al.’s capsule network and the 96.7% CapsNet-Dropout-2 architecture described in Korablyov [Kor17]. Most remarkable, however, is the result that if all the data is provided to the generative capsule network at once, it cannot attain this accuracy—perhaps, a data injection with new information helps the network better sort its information. Maybe networks are not yet perfect at organizing data on their own, and providing data in a certain order, at intervals, can improve learning. Until, of course, the capsule networks learn to do that themselves.

## Acknowledgements

The author would like to thank the Maksym Korablyov and Prof. Joseph Jacobson for their incredible guidance and advice. The author would also like to thank the MIT Media Lab, the MIT PRIMES program, and Derik Kauffman.

## References


Appendix I: The generative capsule architecture

The memo architecture begins with a relatively standard capsule network—we take an input image, convolve it up to the digit capsule layer, and then reconstruct the original image. However, we also use the digit capsules for what we call the memo reconstruction. Namely, we reconstruct ten images, each using the maximal activations of a digit capsule. Using these images, each representing a potential image segmentation, we classify the two digits present in the original image. Thus, instead of minimizing just the margin and reconstruction losses of the original digit capsules, we also minimize the margin and reconstruction losses of the memo. This incentivizes our network to learn segmentation reconstructions that are easy to classify later on, which increases the overall reconstruction quality of our network without sacrificing any accuracy.

The encoder network, shown in Figure 6, is very similar to the encoder network in Sabour et al. [SFH17]. The main difference is that for the multiMNIST dataset, we were able to achieve better performance using two convolutions: the first one with a 9x9 kernel with depth 1 and stride 1 using a LeakyReLU activation and 128 filters, and the second one with a 9x9 kernel with depth 128 and stride 1 using a LeakyReLU activation and 256 filters. The alpha values for the LeakyReLU activations were 0.2 and 0.15, respectively. The Conv2 layer was then convolved up to the PrimaryCaps layer using a similar 9x9 kernel convolution with depth 256, but with stride 2 and a filter size of 32*8, using a normal ReLU activation. Finally, the PrimaryCaps layer is routed to the DigitCaps layer. Analogously to the original paper, we only use routing between two consecutive capsule layers: in this case, the PrimaryCaps and DigitCaps layers.

The image decoder network, shown in Figure 7, uses two convolutional and three fully-connected layers in order to decode the digit capsules back into the 36x36 image. Both convolutions have 3x3 strides, filters of depth 128, and use simple ReLU activations. The three fully connected layers have 2304, 1024, and 1296 neurons, respectively. Applying the two convolutional layers here has an unexpected benefit—although the accuracy does not increase significantly, we achieve state-of-the-art performance over three times faster than an analogous network containing only fully-connected layers. However, convolutional reconstruction has an issue of instability, which we discuss in the results section.

The memo decoder network, shown in Figure 8, is the fundamental part of the memo architecture. We create ten one-hot encodings of the digit caps, one with each capsule activated. Applying three fully-connected layers for reconstruction, we get a [36x36x10] tensor containing a reconstruction attempt for each digit. The best two of ten are combined into the final reconstructed image.

Finally, we reach the last encoding part of the network—the conversion of the memo images to the digit capsules. As shown in Figure 9, we start out by applying the same convolutions up to the Primary Caps layer as in the very beginning of the network. However, instead of using the usual algorithm for getting digit capsules from the primary capsule layer, we use a 1024-neuron fully connected layer, followed by a dropout of 0.5, and followed by a 160-neuron fully connected layer. The result of this layer is then reshaped into the [16x10] digit capsules tensor. It is important to note that, since there are no consecutive capsule layers in this encoder, no routing takes place! The memo encoder uses capsules exclusively for their activations without optimizing agreement.

5.1 Pre-training

When training our network, we utilize a strategy called pre-training: for the first 1000 iterations or so, only the margin and reconstruction loss of the first encoder-decoder is minimized. After the 1000 iterations, both the main loss and the memo loss are minimized. This allows the network to start out with a reasonable accuracy in the first encoder, which significantly accelerates the improvement rate from the addition of the memo decoder-encoder.

5.2 Training

As shown in Figure 10, we use two AdamOptimizers in order to minimize loss [KB14]. The train margin loss is based on the margin loss described in Sabour et al., as shown in Eq. 1.

\[ L_k = T_k \max(0, m^+ - ||v_k||)^2 + \lambda (1 - T_k) \max(0, ||v_k|| - m^-)^2 \] (1)
The reconstruction loss is simply the total squared difference between the reconstructed image and the original. The training AdamOptimizer's loss consists of the margin loss plus the reconstruction loss scaled by a factor of 0.005. The memo AdamOptimizer's loss consists of the margin loss from the reconstruction classification, plus the second reconstruction loss scaled by a factor of 0.005. Both optimizers are trained concurrently, except for the pretraining period described in Section 5.1.
Testing accuracy after low-data injections

Figure 5: Caption in landscape to a figure in landscape.
Figure 6: The encoder network—using two convolutional layers and two capsule layers, it convolves a multiMNIST image up to the DigitCaps layer.

Figure 7: The image decoder network. Using two convolutional and three fully-connected layers, it converts the digit capsules back into a 36x36 image.

Figure 8: The memo decoder network, which decodes every capsule activation to see which digits are present.

Figure 9: The final memo encoder, which convolves from the memo back to the digit capsules. Although not shown in the diagram, the depth of the first convolution is 11, in order to see all of the capsule reconstructions, and not just one at a time.
Figure 10: The full memo architecture, with two encoders and two decoders. Losses in **black** are trained with the Training AdamOptimizer, while ones in **green** are trained using the Memo AdamOptimizer. As in the original paper, the reconstruction losses are scaled by a factor of 0.005 as to not dominate the error term. Finally, it is important to note that the reconstruction loss acts as a regularizer over the network.